Cryptography and Network Security Chapter 13

Fifth Edition

by William Stallings

Chapter 13 – Digital Signatures

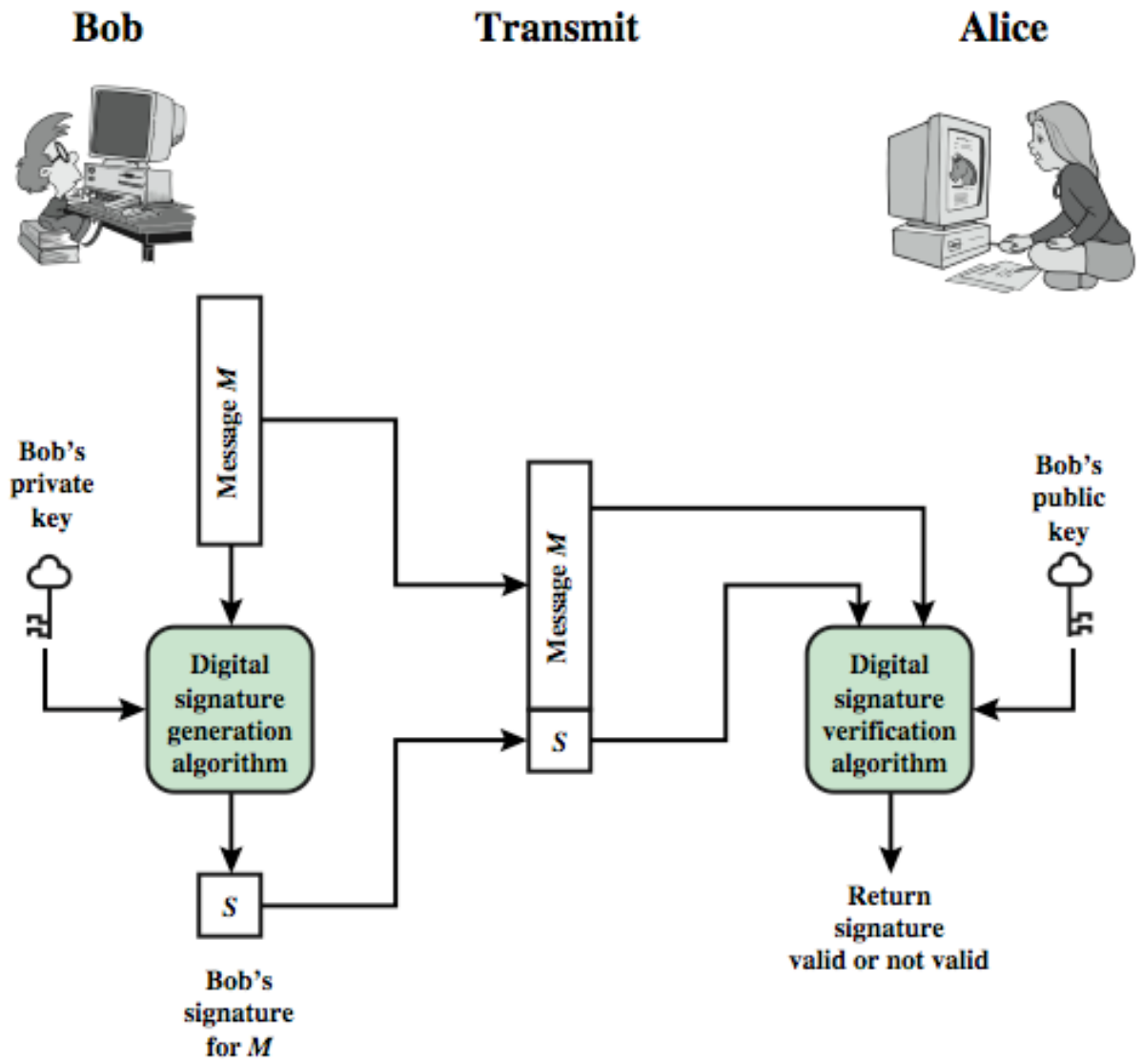
To guard against the baneful influence exerted by strangers is therefore an elementary dictate of savage prudence. Hence before strangers are allowed to enter a district, or at least before they are permitted to mingle freely with the inhabitants, certain ceremonies are often performed by the natives of the country for the purpose of disarming the strangers of their magical powers, or of disinfecting, so to speak, the tainted atmosphere by which they are supposed to be surrounded.

—*The Golden Bough*, Sir James George Frazer

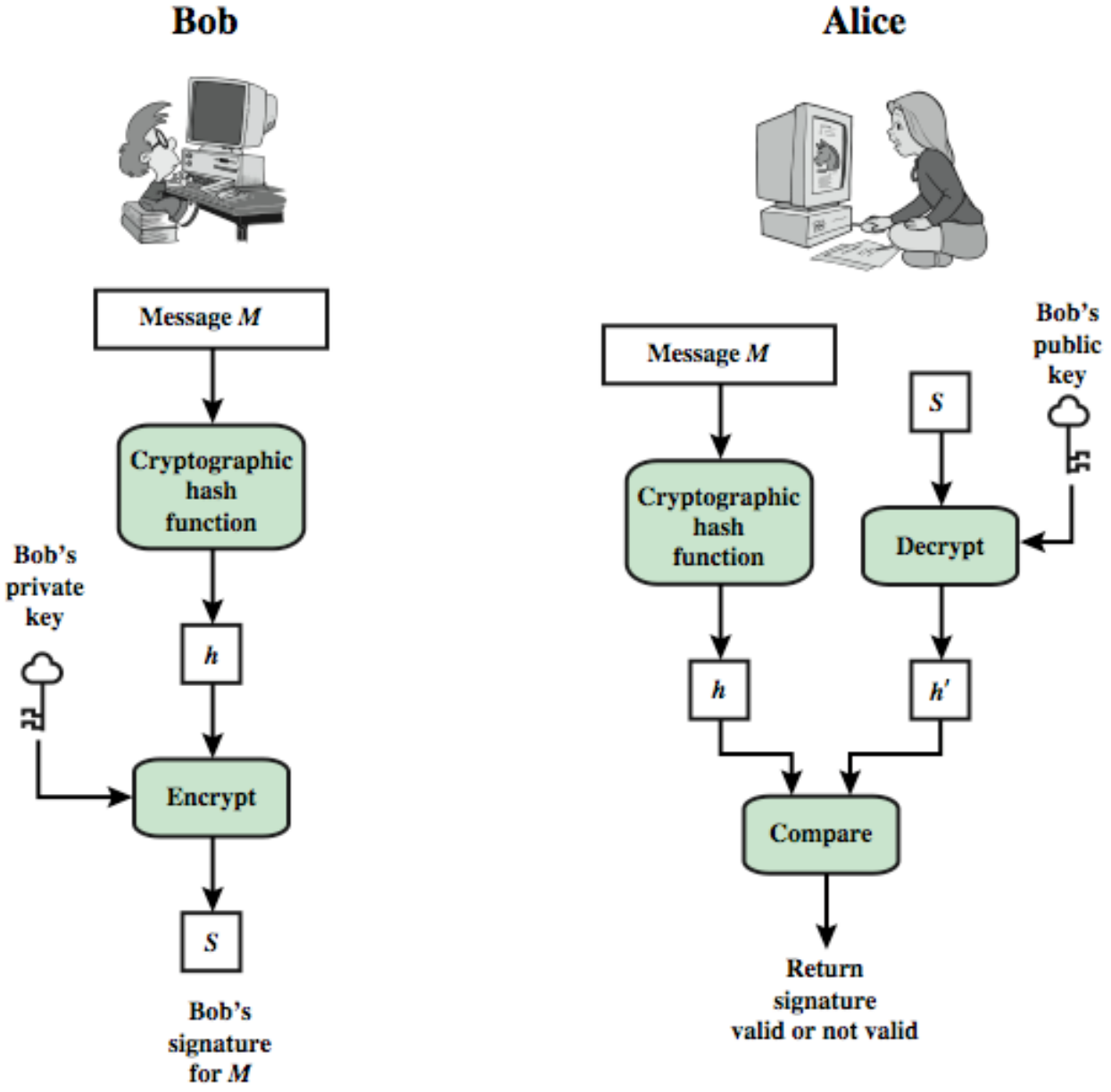
Ψηφιακες Υπογραφες (Digital Signatures)

- Οι ψηφιακες υπογραφες δινουν τη δυνατοτητα:
  - Να επιβεβαιωσουμε τον συντακτη του μηνυματος, την ημερομηνια και την ωρα της υπογραφης
  - Να επιβεβαιωσουμε το περιεχομενο του μηνυματος.
  - Να υπαρχει επιβεβαιωση απο τριτα μερη για να επιλυονται τυχον διαφορες

Μοντελο Ψηφιακης Υπογραφης



Μοντελο Ψηφιακης Υπογραφης



Επιθεσεις και Πλαστογραφιες

- **Επίθεση με γνωση μονο του δημοσιου κλειδιου (key-only attack):** Ο επιτιθεμενος γνωριζει μονο το δημοσιο κλειδι του Α.
- **Επιθεση γνωστου μηνυματος (known message attack):** Ο επιτιθεμενος εχει προσβαση σε μια λιστα μηνηματων και στις υπογραφες τους
- **Επιθεση γενικου επιλεγμενου μηνυματος (generic chosen message attack):** Ο επιτθεμενος επιλεγει μια λιστα μηνυματων πριν προσπαθησει να σπασει το σχημα υπογραφης, ανεξαρτητα απο το δημοσιο κλειδι του Α. Προσπαθει να παρει απο τον Α υπογραφες για τα επιλεγμενα μηνυματα.
- **Επιθεση κατευθυνονενου επιλεγμενου μηνυματος (directed chosen message attack):** Ιδια με την προηγουμενη, αλλα η λιστα των μηνυματων που πρεπει να υπογραφουν επιλεγεται αφου ο επιτιθεμενος λαβει γνωση του δημοσιου κλειδιου του Α, αλλα χωρις να εχει δει οποιαδηποτε υπογραφη.
- **Προσαρμοστικη επιθεση επιλεγμενου μηνυματος (adaptive chosen message attack):** Ο επιτιθεμενος μπορει να χρησιμοποιει τον Α σαν «μαντειο». Μπορει να ζητα υπογραφες απο μηνυματα που εξαρτωνται απο γνωστα απο πριν ζευγη μηνυματος-υπογραφης.

Επιθεσεις και Πλαστογραφιες

- Επιπεδα επιτυχιας «σπασιματος»
  - **Ολικο σπασιμο (total break):** Ο επιτιθεμενος αποκτα γνωση του ιδιωτικου κλειδιου του Α.
  - **Γενικη Πλαστογραφια (universal forgery):** Ο επιτιθεμενος βρισκει εναν ισοδυναμο τροπο να παραγει υπογραφες σε οποιοδηποτε μηνυμα.
  - **Επιλεκτικη Πλαστογραφια (selective forgery):** Ο επιτιθεμενος πλαστογραφει μια υπογραφη για ενα συγκεκριμενο μηνυμα που επιλεγει αυτος.
  - **Πλαστογραφηση υπάρχοντος μηνύματος (existential forgery):** Ο επιτιθεμενος πλαστογραφει τουλαχιστον ενα μηνυμα, χωρις να εχει ελεγχο για το ποιο θα ειναι το μηνυμα.

Απαιτησεις Ψηφιακης Υπογραφης

- Πρεπει να εξαρταται απο το μηνυμα που υπογραφεται
- Πρεπει να χρησιμοποιει πληροφορια μοναδικη για τον υπογραφοντα
  - Για να αποφευχθει η πλαστογραφηση και η αρνηση
- Πρεπει να μπορει να παραχθει σχετικα ευκολα
- Πρεπει να μπορει να αναγνωριστει και να επιβεβαιωθει σχετικα ευκολα
- Πρεπει να ειναι υπολογιστικα ανεφικτο να πλαστογραφηθει
  - Να βρεθει νεο μηνυμα που να ταιριαζει σε υπαρχουσα υπογραφη
  - Να βρεθει υπογραφη για ενα κατασκευασμενο μηνυμα
- Πρεπει να ειναι ευκολο να αποθηκευτει η ψηφιακη υπογραφη σε αποθηκευτικο μεσο

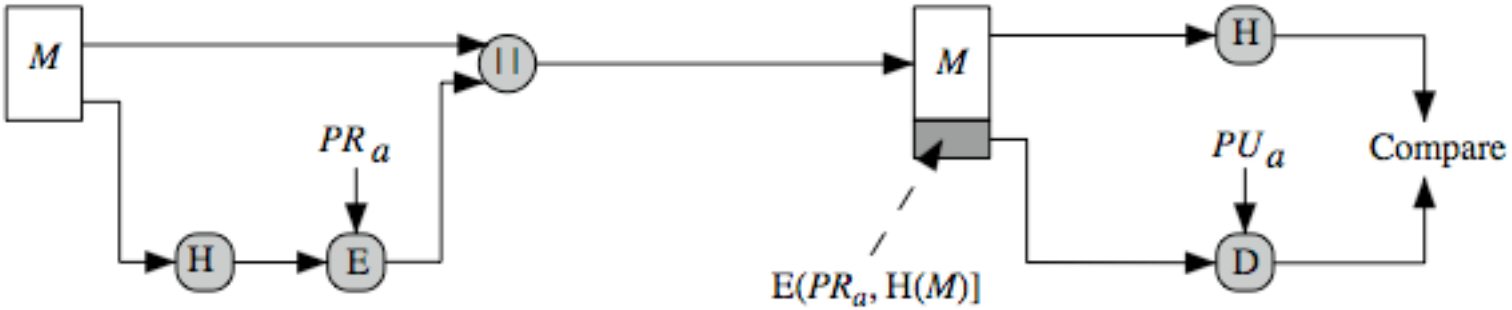
Αμεσες Ψηφιακες Υπογραφες (Direct Digital Signatures)

- Εμπλεκουν μονο τον αποστολεα (υπογραφοντα) και τον παραληπτη
- Προϋποθετουν οτι ο αποδεκτης γνωριζει το δημοσιο κλειδι του αποστολεα
- Η ψηφιακη υπογραφη δημιουργειται απο τον αποστολεα υπογραφοντας με το δημοσιο κλειδι του, ειτε ολοκληρο το μηνυμα, ειτε ενα hash αυτου.
- Μπορει να κρυπτογραφηθει χρησιμοποιωντας το δημοσιο κλειδι του αποδεκτη
- Ειναι σημαντικο να γινει πρωτα η υπογραφη και μετα η κρυπτογραφηση μηνυματος και υπογραφης
- Η ασφαλεια εξαρταται απο το ιδιωτικο κλειδι του αποστολεα

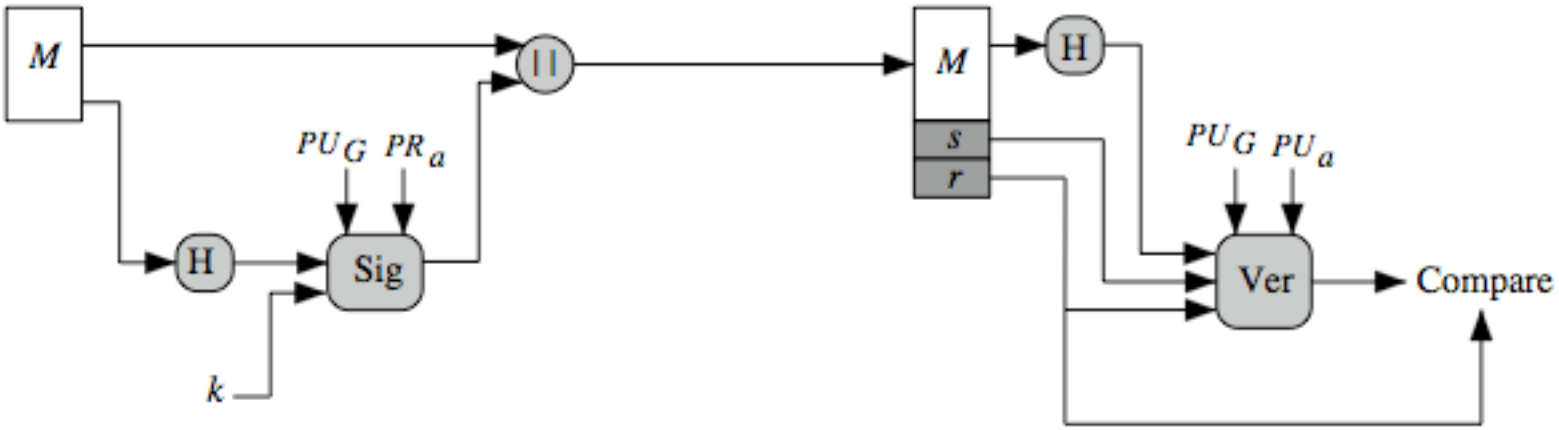
Digital Signature Standard (DSS)

- Εχει εγκριθει απο την κυβερνηση των ΗΠΑ
- Σχεδιαστηκε απο NIST & NSA τη δεκαετια του ‘90
- Δημοσιευτηκε το 1991 και αναθεωρηθηκε το 1993, το 1996 και το 2000
- Χρησιμοποιει το αλγοριθμο hash SHA
- Το standard ονομαζεται DSS και ο αλγοριθμος DSA
- Χρησιμοποιει μια τεχνικη δημοσιου κλειδιου
- Ο DSA σε αντιθεση με τον RSA χρησιμοποιειται μονο για ψηφιακες υπογραφες

DSS vs RSA Signatures



(a) RSA Approach



(b) DSS Approach

Digital Signature Algorithm (DSA)

- Δημιουργει μια υπογραφη των 320 bits
- Με ασφαλεια 512-1024 bit
- Μικροτερος και ταχυτερος απο τον RSA
- Χρησιμοποιειτα μονο για ψηφ.υπογραφες
- Η ασφαλεια του βασιζεται στη δυσκολια να υπολογιστουν διακριτοι λογαριθμοι

Δημιουργια Κλειδιου DSA

- Ειναι γνωστες σε ολους οι τιμες των ολικων δημοσιων κλειδιων (p,q,g):
  - Επιλεγουμε εναν πρωτο αριθμο q των 160-bits
  - Επιλεγουμε εναν μεγαλο πρωτο αριθμο p τετοιο ωστε: $2^{L-1} < p < 2^{L}$
    - οπου L= 512 ως 1024 bits και ειναι πολλαπλασιο του 64
    - Και ο q εχει μηκος 160 bit και ειναι πρωτος διαιρετης του $(p-1)$
  - Επιλεγουμε $g = h^{(p-1)/q}$
    - οπου $1<h<p-1$ και $h^{(p-1)/q} \bmod p > 1$
- Οι χρηστες επιλεγουν το ιδιωτικο και υπολογιζουν το δημοσιο κλειδι τους:
  - Επιλεγεται τυχαια το ιδιωτικο κλειδι: $x<q$
  - Υπολογιζεται το δημοσιο κλειδι: $y = g^{x} \bmod p$

Δημιουργια Υπογραφης DSA

- Για να υπογραφει ενα μηνυμα M ο αποστολεας (υπογραφων):
  - Δημιουργει ενα τυχαιο κλειδι υπογραφης k, k<q
  - Το k πρεπει να ειναι τυχαιο, να καταστρεφεται μετα τη χρηση και να μην ξαναχρησιμοποιειται
- Στη συνεχεια υπολογιζεται το ζευγος υπογραφης:

  $r = (g^k \bmod p) \bmod q$

  $s = [k^{-1}(H(M) + xr)] \bmod q$
- Στελνεται η υπογραφη(r,s) μαζι με το μηνυμα M

Επιβεβαιωση Υπογραφης DSA

- Εχοντας λαβει το μηνυμα M και την υπογραφη(r,s)
- Για να **επιβεβαιωσει** την υπογραφη ο αποδεκτης υπολογιζει:

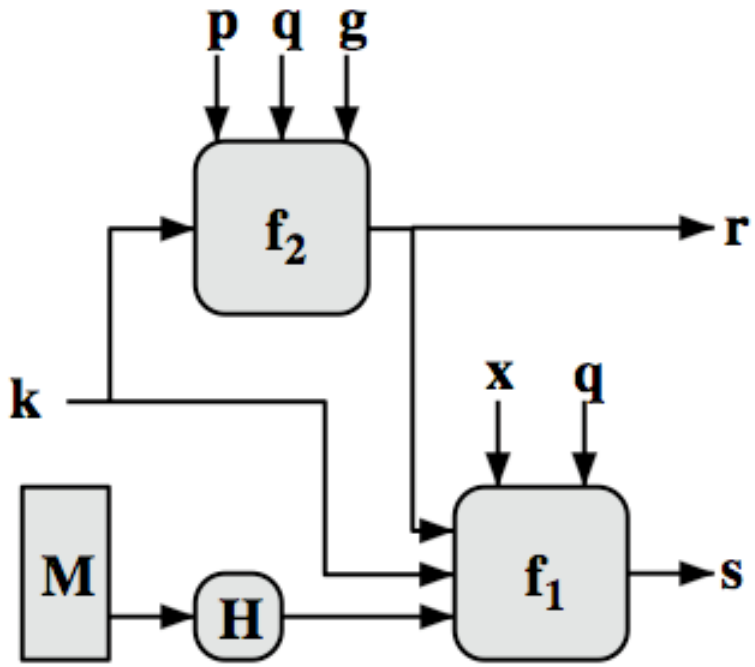
  $w = s^{-1} \bmod q$

  $u1 = [H(M)w] \bmod q$

  $u2 = (rw) \bmod q$

  $v = [(g^{u1}\ y^{u2}) \bmod p] \bmod q$
- Αν v=r τοτε η υπογραφη επιβεβαιωνεται

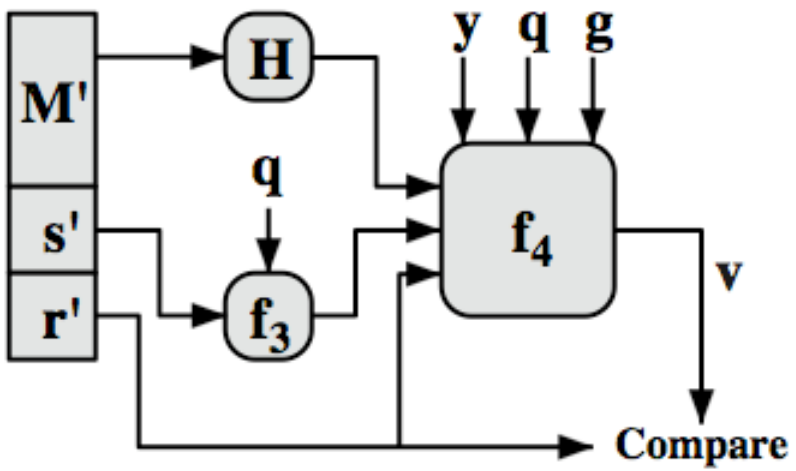
DSS Overview



$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing



$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r')$

$= ((g^{(H(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Συνοψη

- Εξετασαμε:
  - Τις ψηφιακες υπογραφες
  - Τον αλγοριθμο DSA και το προτυπο DSS